

Beleidskader Cameratoezicht Erasmus Universiteit Rotterdam 2026-2031

Dit beleidsdocument is vastgesteld door het College van Bestuur op 22 september 2026.
Dit beleidsdocument heeft instemming verkregen van de Universiteitsraad op 16 juli 2026.
Dit beleidsdocument treedt in werking op 1 oktober 2026.

Afdeling : ABD, BZ, Integrale Veiligheid

Versie : 0.44NL

Inhoudsopgave

1	Inleiding en scope.....	2
2	Doelstelling cameratoezicht.....	3
2.1	<i>Werking en inzet.....</i>	3
2.2	<i>Reikwijdte en begrenzing van de inzet.....</i>	3
3	Soorten cameratoezicht.....	4
3.1	<i>Permanent cameratoezicht.....</i>	4
3.1.1	<i>Vaste camera's.....</i>	4
3.1.2	<i>PTZ-camera's.....</i>	4
3.1.3	<i>Kentekenherkenning.....</i>	4
3.2	<i>Tijdelijk aanvullend cameratoezicht.....</i>	5
3.3	<i>Heimelijk cameratoezicht.....</i>	5
4	Criteria en uitgangspunten voor cameratoezicht.....	7
4.1	<i>Generieke procedure voor aanvragen cameratoezicht.....</i>	7
4.2	<i>Locatiecategorieën voor cameratoezicht.....</i>	8
4.2.1	<i>Locaties met structurele noodzaak voor cameratoezicht.....</i>	8
4.2.2	<i>Locaties waar cameratoezicht onder voorwaarden is toegestaan.....</i>	10
4.2.3	<i>Locaties waar cameratoezicht in beginsel niet is toegestaan.....</i>	11
4.2.4	<i>Locaties waar cameratoezicht nooit is toegestaan.....</i>	11
4.3	<i>Externe EUR-locaties (ISS, EUC, C&C Putselaan).....</i>	11
5	Privacy en waarborgen.....	12
5.1	<i>Verwerkingsgrondslag.....</i>	12
5.2	<i>Waarborgen.....</i>	12
6	Werking en Evaluatie.....	15
6.1	<i>Interpretatie.....</i>	15
6.2	<i>Beheer.....</i>	15
6.3	<i>Vertaling.....</i>	15
6.4	<i>Inwerkingtreding, werkingsduur, en evaluatie.....</i>	15
6.5	<i>Citeertitel.....</i>	15
	Bijlage 1 – Autorisatiematrix.....	16

1 Inleiding en scope

De campus van de Erasmus Universiteit Rotterdam (EUR) heeft een open en toegankelijk karakter. Om dit karakter te behouden en tegelijkertijd de veiligheid te waarborgen, zet de EUR al vele jaren cameratoezicht in als onderdeel van een brede veiligheidsaanpak. Camera's worden op specifieke plaatsen op de campus geplaatst om de veiligheid te vergroten.

De EUR ziet cameratoezicht niet als oplossing voor alle veiligheidsvraagstukken, en zeker niet als een doel op zich. Cameratoezicht is altijd onderdeel van een breder pakket aan veiligheidsmaatregelen, zoals regelmatige surveillancerondes, goede verlichting en open zichtlijnen. Dit totale pakket aan maatregelen valt buiten de reikwijdte van dit beleidskader, dat specifiek toeziet op cameratoezicht. De mogelijkheid om alternatieve maatregelen te nemen heeft wel implicaties voor dit kader: bij de plaatsing van camera's weegt de EUR noodzaak, proportionaliteit en subsidiariteit altijd expliciet af.

De EUR erkent dat er een inherent spanningsveld bestaat tussen cameratoezicht en het recht op eerbiediging van de persoonlijke levenssfeer. Een zekere inbreuk op de persoonlijke levenssfeer van studenten, medewerkers en bezoekers wordt noodzakelijk geacht om te kunnen voldoen aan de zorgplicht voor hun veiligheid. De EUR maakt daarbij steeds een zorgvuldige afweging tussen het na te streven doel enerzijds en de gevolgen voor de persoonlijke levenssfeer anderzijds, en treft maatregelen om de impact van cameratoezicht zoveel mogelijk te beperken.

Dit beleidskader licht toe waarom en hoe de EUR cameratoezicht inzet en is van toepassing op alle terreinen en gebouwen van de EUR. Met dit beleidskader streeft de EUR ernaar dat inzet van cameratoezicht voorspelbaar, transparant en uitlegbaar is. Ook worden voorwaarden gesteld waarbinnen de EUR cameratoezicht kan inzetten. Daarnaast gaat dit beleidskader in op de waarborgen die de EUR treft om de impact van cameratoezicht op de persoonlijke levenssfeer te beperken. De formele processen en governance zijn vastgelegd in het Reglement Cameratoezicht EUR 2026.

Dit beleidskader en het Reglement Cameratoezicht EUR 2026 vormen samen het kader voor de inzet van cameratoezicht op de EUR. In dit beleidskader worden met name de doelstellingen, criteria en locatiecategorieën voor de plaatsing en inzet van camera's beschreven; het Reglement bevat de procedurele uitwerking en de voorwaarden voor de verwerking van camerabeelden en andere gegevens. Dit beleidskader richt zich uitsluitend op cameratoezicht ter bevordering van veiligheid in de gebouwen en op de terreinen van de EUR. Andere vormen van cameragebruik, bijvoorbeeld ten behoeve van onderwijs, onderzoek of bedrijfsvoering, vallen buiten de reikwijdte van dit beleidskader.

2 Doelstelling cameratoezicht

Cameratoezicht wordt ingezet ter bescherming van de veiligheid en gezondheid van studenten, medewerkers en derden, ter beveiliging van de toegang tot en het gebruik van gebouwen en terreinen van de EUR, en ter bescherming van eigendommen van de EUR. Daarnaast draagt cameratoezicht bij aan het voorkomen, signaleren en beëindigen van incidenten. De EUR realiseert deze doelstellingen door het nemen van een breed scala aan veiligheidsmaatregelen, waarvan cameratoezicht een belangrijk onderdeel vormt.

2.1 Werking en inzet

Cameratoezicht wordt in beginsel primair ingezet ter preventie van incidenten. De zichtbare aanwezigheid van camera's kan potentiële overtredingen en ongewenst gedrag ontmoedigen en draagt daarmee bij aan het voorkomen van incidenten. Daarnaast stelt cameratoezicht de beveiligingsdienst in staat om afwijkende of risicovolle situaties vroegtijdig te signaleren en, waar nodig, preventief in te grijpen.

Cameratoezicht ondersteunt daarnaast de directe interventie bij incidenten: camerabeelden kunnen worden gebruikt om situaties te beoordelen, de inzet van beveiligingsmedewerkers te sturen, passende maatregelen te treffen en, waar nodig, hulpdiensten tijdig en effectief te informeren en te begeleiden. Na afloop van een incident kunnen camerabeelden worden ingezet ter vaststelling van de toedracht en, indien van toepassing, ter ondersteuning van opsporing en vervolging.

De aanwezigheid van cameratoezicht kan voorts bijdragen aan het ervaren veiligheidsgevoel van studenten, medewerkers en bezoekers, mits cameratoezicht zichtbaar, proportioneel en transparant wordt toegepast. Een toename van het veiligheidsgevoel vormt echter nooit het primaire doel voor de plaatsing van camera's; zonder aanvullende maatregelen zou dit leiden tot schijnveiligheid.

2.2 Reikwijdte en begrenzing van de inzet

De inzet van cameratoezicht door de EUR is begrensd door het recht op eerbiediging van de persoonlijke levenssfeer en andere fundamentele rechten en vrijheden van studenten, medewerkers en bezoekers. De EUR maakt daarom bij ieder besluit tot inzet van cameratoezicht een zorgvuldige afweging tussen enerzijds de te beschermen veiligheidsbelangen en anderzijds de gevolgen voor de persoonlijke levenssfeer.

Cameratoezicht wordt uitsluitend ingezet ter bevordering van de veiligheid en de orde op de gebouwen en terreinen van de EUR en heeft uitdrukkelijk niet tot doel om rechten en vrijheden van studenten en medewerkers – zoals de vrijheid van meningsuiting en het recht van vergadering en betoging – te beperken. Een concreet voorbeeld is cameratoezicht bij manifestaties: dit wordt ingezet om de veiligheid van alle aanwezigen, inclusief de deelnemers, te waarborgen en niet om het demonstratierecht of andere fundamentele vrijheden te beperken.

3 Soorten cameratoezicht

De EUR maakt gebruik van meerdere vormen van cameratoezicht. In de basis gebruikt de EUR permanente en zichtbare camera's. Indien de omstandigheden daartoe aanleiding geven, kan de EUR daarnaast tijdelijk aanvullend cameratoezicht inzetten, bijvoorbeeld in de vorm van mobiele camera's. Tijdelijk aanvullend cameratoezicht wordt op basis van dezelfde criteria en waarborgen ingezet als het permanente cameratoezicht en onderscheidt zich met name door de beperkte duur van de inzet en de technische uitwerking. In zeer uitzonderlijke gevallen kan de EUR gebruikmaken van heimelijk cameratoezicht. Deze vorm van cameratoezicht kan een grotere inbreuk op de persoonlijke levenssfeer van studenten, medewerkers en bezoekers meebrengen. Om die reden gelden hiervoor extra voorwaarden en aanvullende waarborgen.

3.1 Permanent cameratoezicht

Permanent cameratoezicht wordt ingezet om gedurende langere tijd structureel toezicht te houden op specifieke locaties van de EUR. Dit permanente netwerk vormt de basis van het cameratoezicht op de terreinen en in de gebouwen van de EUR. Camera's worden uitsluitend geplaatst op basis van een risicoanalyse en een toets aan de criteria zoals beschreven in hoofdstuk 4. De procedure voor de besluitvorming en de verwerking van camerabeelden is vastgelegd in het Reglement Cameratoezicht EUR 2026.

Binnen het permanente cameratoezicht maakt de EUR gebruik van verschillende typen camera's, waaronder vaste camera's en PTZ-camera's.

3.1.1 Vaste camera's

Vaste camera's zijn camera's die permanent in één vaste richting zijn gericht en geen actieve besturing kennen. Zij registreren uitsluitend het vooraf vastgestelde beeldgebied. Vaste camera's worden ingezet om continu zicht te houden op specifieke locaties, zoals toegangen tot gebouwen en centrale ruimten op de Campus.

3.1.2 PTZ-camera's

PTZ-camera's (Pan-Tilt-Zoom) zijn camera's die op afstand kunnen worden bestuurd door de centralist in de meldkamer van de beveiliging. Deze camera's kunnen worden gedraaid, gekanteld en ingezoomd en bieden daarmee de mogelijkheid om in te spelen op actuele situaties.

Wanneer een PTZ-camera niet actief wordt bestuurd, functioneert deze als een vaste camera met een vooraf ingestelde kijkrichting. Actieve besturing van een PTZ-camera vindt alleen plaats wanneer daar aanleiding toe is, bijvoorbeeld bij een incident. In dergelijke gevallen kan de camera tijdelijk worden gericht op een andere locatie, bijvoorbeeld om de verplaatsing van een ongewenst persoon op het terrein te volgen of om een onveilige situatie nader te beoordelen.

3.1.3 Kentekenherkenning

Naast het reguliere cameratoezicht in parkeergarages wordt er ook gebruik gemaakt van camera's met kentekenherkenning. Deze camera's zijn geplaatst bij ingangen van parkeergarages op campus Woudestein en worden gebruikt voor betalingsdoeleinden. Omdat deze camera's niet worden ingezet voor cameratoezicht ter bevordering van de veiligheid in de zin van dit beleidskader, vallen zij buiten de reikwijdte hiervan. Voor de verwerking van kentekengegevens gelden afzonderlijke kaders en procedures.

3.2 Tijdelijk aanvullend cameratoezicht

In aanvulling op permanent cameratoezicht kan de EUR gebruikmaken van tijdelijk aanvullend cameratoezicht indien daartoe een concrete noodzaak bestaat. Onder tijdelijk aanvullend cameratoezicht wordt verstaan: de tijdelijke uitbreiding van het bestaande netwerk van camera's op grond van een specifieke dreiging, een verhoogd risico of een bijzondere situatie, wanneer het permanente cameratoezicht onvoldoende dekking of mogelijkheden biedt.

Tijdelijk aanvullend cameratoezicht wordt ingezet om gedurende een vooraf bepaalde periode toezicht te houden op een specifiek gebied of een specifieke locatie. In de praktijk wordt hierbij veelal gebruikgemaakt van mobiele of flexibel inzetbare camera's. Dit kunnen zowel vaste camera's als PTZ-camera's zijn.

Tijdelijk aanvullend cameratoezicht wordt uitsluitend ingezet wanneer zich (dreigende) wanordelijkheden of incidenten voordoen, of wanneer daar op basis van concrete signalen of ervaringen een reële verwachting van bestaat. Daarnaast kan bij evenementen worden besloten tot de inzet van tijdelijk cameratoezicht, indien de aard, omvang of locatie van het evenement daartoe aanleiding geeft. In alle gevallen worden tijdelijke camera's uitsluitend gericht op het betreffende gebied en uitsluitend ingezet voor het doel waarvoor zij zijn geplaatst.

Bij een inzet van tijdelijk aanvullend cameratoezicht worden het doel, de duur en de reikwijdte van het cameratoezicht vooraf gemotiveerd vastgelegd. Na afloop van de vooraf vastgestelde periode wordt het tijdelijk aanvullend cameratoezicht geëvalueerd. Op basis van deze evaluatie kan worden besloten het cameratoezicht te beëindigen, de inzet voor een beperkte periode te verlengen, of, indien sprake is van een structurele noodzaak, over te gaan tot permanent cameratoezicht. De procedure voor inzet van tijdelijk aanvullend cameratoezicht is vastgelegd in het Reglement Cameratoezicht EUR 2026.

3.3 Heimelijk cameratoezicht

Cameratoezicht op de EUR is in beginsel zichtbaar voor iedereen die zich op het terrein of in de gebouwen van de EUR bevindt. Deze zichtbaarheid is wenselijk, omdat zij bijdraagt aan de preventieve werking van cameratoezicht. Slechts in zeer uitzonderlijke gevallen kan de EUR gebruikmaken van heimelijk cameratoezicht. Daarbij volgt de EUR de richtlijnen van de Autoriteit Persoonsgegevens.

Heimelijk cameratoezicht wordt uitsluitend ingezet als *ultimum remedium*. Dit is alleen toegestaan als regulier cameratoezicht en andere door de EUR genomen maatregelen aantoonbaar niet hebben geleid tot het beëindigen van structurele incidenten, én er sprake is van gerede of gegronde vermoedens van strafbare feiten of ander ernstig laakbaar gedrag.

Naast de *Data Protection Impact Assessment* (DPIA) die de EUR uitvoert op het cameratoezicht als geheel, voert de EUR een afzonderlijke DPIA uit specifiek voor heimelijk cameratoezicht als verwerkingscategorie. Deze DPIA is generiek van aard en beschrijft de aanvullende risico's en waarborgen die gelden voor heimelijk cameratoezicht. Bij ieder besluit tot inzet van heimelijk cameratoezicht wordt getoetst of dit besluit past binnen de uitgangspunten en randvoorwaarden van deze generieke DPIA. De in de DPIA beschreven maatregelen omvatten zowel organisatorische als technische waarborgen die zijn gericht op het voorkomen en signaleren van misbruik tijdens de uitvoering, zoals een strikte beperking van de toegang tot camerabeelden tot een kleine, daartoe geautoriseerde groep medewerkers, het vastleggen en periodiek controleren van loggegevens van raadplegingen, en verplichte instructie en geheimhouding voor medewerkers die toegang hebben tot heimelijk cameratoezicht.

Het besluit tot inzet van heimelijk cameratoezicht wordt altijd door het College van Bestuur genomen, conform het Reglement Cameratoezicht EUR 2026. Heimelijk cameratoezicht is altijd tijdelijk van aard; de duur en reikwijdte worden vooraf expliciet begrensd.

Na beëindiging van het heimelijk cameratoezicht worden de Universiteitsraad en de betrokken medewerkers en studenten hierover geïnformeerd, met inachtneming van eventuele beperkingen die kunnen voortvloeien uit lopende onderzoeken of procedures. De procedure voor de inzet van heimelijk cameratoezicht en de verwerking van camerabeelden is vastgelegd in het Reglement Cameratoezicht EUR 2026.

4 Criteria en uitgangspunten voor cameratoezicht

Cameratoezicht brengt een inherent spanningsveld met zich mee tussen veiligheid en de bescherming van de persoonlijke levenssfeer. Om hier zorgvuldig mee om te gaan, hanteert de EUR een vaste methodiek voor de inzet van cameratoezicht. Alle voorstellen worden getoetst aan de criteria noodzaak, proportionaliteit en subsidiariteit, en aan een expliciete privacy-afweging. Cameratoezicht wordt daarbij niet *ad hoc* vormgegeven, maar ingebed in een samenhangend ontwerp van het cameranetwerk: de campus en gebouwen zijn ingedeeld in categorieën van locaties, waarvoor per categorie is vastgelegd of, en onder welke voorwaarden, cameratoezicht kan worden toegepast.

4.1 Generieke procedure voor aanvragen cameratoezicht

De formele procedures rond de aanvraag en beoordeling van cameratoezicht zijn vastgelegd in hoofdstuk IV van het Reglement Cameratoezicht EUR 2026. In de basis worden aanvragen voor de inrichting of wijziging van cameratoezicht beoordeeld door het Toetsingsteam Cameratoezicht.

Het Toetsingsteam Cameratoezicht is een multidisciplinair team dat ten minste bestaat uit de Adviseur Integrale Veiligheid, de Privacy Officer ABD en de Servicemanager Parkmanagement/CCTV van RE&F. Zij brengen respectievelijk de veiligheidsbelangen, de privacybelangen en de technische en facilitaire aspecten in en wegen deze gezamenlijk af. Aanvullend kan de Universiteitsraad ook een eigen vertegenwoordiger aanwijzen om deel te nemen aan het toetsingsteam. Deze vertegenwoordiger is adviserend in het team, en vertegenwoordigd de belangen van studenten en medewerkers op de EUR. Indien nodig kunnen aanvullende deskundigen worden betrokken.

Het Toetsingsteam toetst aanvragen aan de volgende criteria:

- Noodzaak: Voor de plaatsing van een camera of de uitbreiding van het cameratoezicht wordt een duidelijke doelstelling geformuleerd, die past binnen de algemene doelstellingen van cameratoezicht van de EUR. De noodzaak volgt uit een risicoanalyse, uitgevoerd door het team Integrale Veiligheid.
- Proportionaliteit: Het toepassen van cameratoezicht brengt per definitie een inbreuk op de persoonlijke levenssfeer van studenten, medewerkers en bezoekers met zich mee. De aard en omvang van deze inbreuk moeten in redelijke verhouding staan tot het beoogde doel van het cameratoezicht.
- Subsidiariteit: Cameratoezicht wordt alleen ingezet wanneer het beoogde doel niet kan worden bereikt met een minder ingrijpende maatregel, of wanneer dergelijke maatregelen onvoldoende effectief zijn gebleken.
- Expliciete belangenafweging: Ook maakt de EUR een expliciete belangenafweging. Daarin worden de belangen van de EUR op het gebied van veiligheid, orde en eigendomsbescherming afgewogen tegen de belangen van betrokkenen. In de basis worden deze belangen in kaart gebracht in de Legitimate Interest Assessment (LIA) als onderdeel van de Data Protection Impact Assessment (DPIA) die wordt uitgevoerd voor het gehele cameratoezichtssysteem. Bij concrete besluiten over cameratoezicht wordt getoetst of deze passen binnen de belangen, uitgangspunten en waarborgen zoals in de LIA en DPIA geformuleerd. De vertegenwoordiger van de Universiteitsraad kan in het bijzonder advies geven over de geraakte belangen van betrokkenen.

Het Toetsingsteam Cameratoezicht brengt naar aanleiding van de beoordeling een advies uit over de gevraagde inzet van cameratoezicht. Dit advies wordt marginaal getoetst door de Chief Privacy Officer. Indien noodzakelijk kan de Functionaris Gegevensbescherming een bindend advies uitbrengen.

4.2 Locatiecategorieën voor cameratoezicht

Om de algemene criteria uit paragraaf 4.1 consequent toe te passen, hanteert de EUR een indeling in locatiecategorieën. Daarbij wordt uitgegaan van het idee dat cameratoezicht op sommige plekken structureel onderdeel is van de veiligheidsinrichting, terwijl het op andere plekken slechts na een concrete risicoanalyse kan worden ingezet, in weer andere situaties alleen in zeer uitzonderlijke gevallen kan worden overwogen, en op bepaalde plekken helemaal niet passend is.

Deze systematiek voorkomt *ad hoc* beslissingen en maakt de toepassing van cameratoezicht voorspelbaar, transparant en uitlegbaar. In de paragrafen 4.2.1 tot en met 4.2.4 worden deze categorieën verder uitgewerkt.

4.2.1 Locaties met structurele noodzaak voor cameratoezicht

Dit zijn locaties waar cameratoezicht altijd of structureel wordt toegepast, omdat bij de inrichting van de veiligheidsmaatregelen is vastgesteld dat dit een noodzakelijke maatregel is binnen de bredere veiligheidsaanpak van de EUR. Voor deze locaties is in generieke zin onderbouwd dat cameratoezicht noodzakelijk, proportioneel en subsidiair is, en dat de privacy-afweging aanvaardbaar is; deze onderbouwing is vastgelegd in dit beleidskader, de LIA en de DPIA voor het cameratoezicht.

Bij voorstellen voor nieuwe of aangepaste cameraposities op deze locaties wordt niet telkens opnieuw een volledige (belangen)afweging gemaakt. De beoordeling richt zich erop of:

- de beoogde camera past binnen de generieke doelstellingen, reikwijdte en waarborgen voor deze categorie; en
- er geen bijzondere omstandigheden zijn die zich tegen plaatsing op de betreffende locatie verzetten.

Binnen deze categorie vallen in ieder geval de volgende typen locaties:

Toegangen en buitenruimten Campus Woudestein en gebouwen

Het terrein van Campus Woudestein en de gebouwen daarop hebben een openbaar karakter, met meerdere fysieke toegangswegen en open verbindingen met de openbare ruimte. In de praktijk maakt dit het moeilijk om ongewenste bezoekers tijdig te signaleren. Dit belemmert zowel de preventie van incidenten, omdat vroegtijdig ingrijpen door de beveiligingsdienst daardoor lastiger wordt, als de mogelijkheid tot opsporing en afdoening achteraf, doordat vaak geen bruikbaar beeldmateriaal beschikbaar is.

Om deze risico's te beperken, en tegelijk het open karakter van de campus en gebouwen zo veel mogelijk te behouden, plaatst de EUR vaste camera's bij alle toegangswegen tot het terrein en bij de in- en uitgangen van gebouwen. Deze camera's zijn gericht op de directe toegangszones en niet op verblijfsruimten. Zij worden niet gebruikt om het gedrag van individuele personen gedurende langere tijd te volgen, maar uitsluitend om inzicht te krijgen in wie het terrein en de gebouwen betreedt en verlaat ten behoeve van veiligheid en incidentafhandeling.

Alternatieve maatregelen, zoals intensievere surveillance of extra fysieke barrières, zijn alleen effectief tegen hogere kosten en met een grotere impact op de toegankelijkheid en het gebruik van de campus. Vanuit het subsidiariteitsbeginsel wordt cameratoezicht daarom ingezet als aanvullende maatregel, in combinatie met bestaande maatregelen zoals verlichting, inrichting van looproutes en de aanwezigheid van beveiligingsmedewerkers.

Centrale buitenruimten en gebieden tussen gebouwen op Campus Woudestein

Ook maakt de EUR op het campusterrein gebruik van een samenhangend netwerk van camera's, waarbij blinde vlekken zo veel mogelijk worden beperkt. Campus Woudestein is qua oppervlakte en aantal gebouwen dermate groot dat effectief toezicht door uitsluitend fysieke aanwezigheid van beveiligingsmedewerkers niet haalbaar is. Het cameranetwerk stelt de beveiligingsdienst in staat om tijdens een incident snel een adequaat beeld van de situatie te krijgen, zodat passende maatregelen kunnen worden getroffen en hulpdiensten waar nodig gericht kunnen worden aangestuurd.

Het netwerk van vaste camera's en PTZ-camera's maakt het mogelijk dat de centralist bij een incident gericht zicht kan krijgen op de situatie, bijvoorbeeld door een PTZ-camera op de betreffende locatie te richten. Daarnaast kan dit netwerk in uitzonderlijke situaties worden gebruikt om, uitsluitend handmatig en niet via AI-gestuurde systemen, een persoon gedurende een beperkte periode over (een deel van) het terrein te volgen. Dit is alleen toegestaan bij een concrete aanleiding en redelijke verdenking, voor zover noodzakelijk voor de in dit beleid vastgestelde doelen van cameratoezicht, bijvoorbeeld bij ernstig ongewenst of dreigend gedrag of wanneer een verdachte situatie zich verplaatst over de campus. Het volgen wordt beperkt tot de relevante route en periode en wordt niet gebruikt voor structurele gedragsmonitoring van individuele personen.

Een alternatief, zoals structureel meer beveiligingsmedewerkers op het terrein inzetten of (tijdelijk) delen van de campus afsluiten, zou een grotere impact hebben op de dagelijkse toegankelijkheid en het gebruik van de campus en biedt daarbij niet dezelfde mate van overzicht en handelingssnelheid. Tegen deze achtergrond wordt het samenhangende cameranetwerk op Campus Woudestein beschouwd als een noodzakelijke en, in verhouding tot de risico's en beschikbare alternatieven, proportionele maatregel.

Parkeergarages

In de parkeergarages van de EUR wordt een dekkend netwerk van CCTV-camera's ingezet. Dit netwerk heeft een tweeledig doel. Primair dient het ter bescherming van personen bij calamiteiten: het biedt direct inzicht in de situatie en maakt het mogelijk vast te stellen of er nog aanwezigen zijn, bijvoorbeeld bij brand of een andere noodsituatie. Daarnaast draagt het cameranetwerk bij aan het terugdringen van vermogensdelicten, zoals diefstal en vandalisme. Onderzoek op vergelijkbare locaties laat zien dat cameratoezicht in parkeergarages een relevant preventief effect kan hebben op dergelijke incidenten.¹

Bedrijfskritische IT-infrastructuur

Binnen het cameratoezicht van de EUR is in het bijzonder aandacht voor bedrijfskritische IT-infrastructuur. Het gaat hierbij onder meer om datacenters en overige als bedrijfskritisch geclassificeerde IT-voorzieningen. Bij deze locaties wordt standaard cameratoezicht toegepast. EIDS en Integrale Veiligheid stellen deze classificatie gezamenlijk vast.

Het primaire doel hiervan is het waarborgen en versterken van de informatiebeveiliging. Cameratoezicht draagt bij aan het voorkomen, detecteren en onderzoeken van ongeautoriseerde toegang en vormt daarmee een belangrijk onderdeel van de fysieke beveiligingsmaatregelen rond bedrijfskritische IT-infrastructuur. Daarnaast acht de EUR dit cameratoezicht noodzakelijk voor compliance met de ISO-27001/27002-normering en de daarmee samenhangende eisen ten aanzien van fysieke beveiliging van datacenters en overige kritieke IT-voorzieningen.

Gezien de specifieke functie van deze ruimten, de strikt beperkte toegang en het feit dat zij uitsluitend worden betreden voor technische en beheersmatige werkzaamheden, is de impact op de persoonlijke levenssfeer van medewerkers en studenten beperkt.

¹ Zie bijvoorbeeld: Piza, E.L., Welsh, B.C., Farrington, D.P., & Thomas, A.L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>

4.2.2 Locaties waar cameratoezicht onder voorwaarden is toegestaan

Dit zijn locaties waar cameratoezicht niet standaard wordt toegepast, maar waar het, afhankelijk van de omstandigheden, een passende maatregel kan zijn. Voor iedere camera wordt afzonderlijk een risicoanalyse uitgevoerd en een expliciete afweging gemaakt of cameratoezicht noodzakelijk, proportioneel en subsidiair is. Daarbij wordt getoetst of de in de LIA en de DPIA opgenomen belangenafweging en waarborgen de beoogde inzet voldoende dekken, of dat aanvullende maatregelen nodig zijn. De besluitvorming over cameratoezicht op deze locaties vindt plaats volgens de procedure van artikel 4.2 van het Reglement Cameratoezicht EUR 2026.

Binnen deze categorie vallen in ieder geval de volgende typen locaties:

Cameratoezicht in gebouwen: centrale ruimten en toegang tot kantoorgebieden

Binnen de gebouwen van de EUR wordt cameratoezicht terughoudend toegepast. De EUR maakt hierin een bewuste afweging tussen veiligheid, privacy en het behoud van een open en prettig werk- en studeerklimaat. Hoewel zich in het verleden incidenten hebben voorgedaan, zoals diefstal en inbraak, waarbij een uitgebreider cameranetwerk mogelijk had kunnen bijdragen aan het vergaren van bewijsmateriaal, weegt dit voor de EUR niet op tegen de negatieve gevolgen van een grootschalige inzet van camera's binnen gebouwen.

Aanvullend op camera's bij in- en uitgangen kan de EUR cameratoezicht inzetten in centrale ruimten binnen gebouwen, zoals centrale entreehallen en publieksruimten bij collegezalen (*nota bene* niet de collegezalen zelf), hoofdgangen, trappenhuizen en lifthallen. Deze inzet is primair gericht op het houden van zicht op personenstromen en het tijdig signaleren van incidenten.

In kantoorgebieden waar een verhoogd risico bestaat op ongeoorloofde toegang kan de EUR cameratoezicht toepassen bij de toegang. Dit cameratoezicht maakt altijd deel uit van een bredere set beveiligingsmaatregelen, zoals beschreven in het toegangs- en compartimenteringsbeleid van de EUR. De EUR draagt er daarbij zorg voor dat uitsluitend de toegang tot het kantoorgebied wordt gefilmd en niet de aangrenzende werkplekken. Dergelijke cameraposities kunnen eveneens worden gerealiseerd op gemotiveerd verzoek van een beheerder ten behoeve van diens dienst of faculteit.

Overige risicovolle gebieden

Daarnaast zijn er specifieke gebieden waar een verhoogd risico bestaat op incidenten, vermogensdelicten of ongeoorloofde toegang, en waar cameratoezicht een passende aanvullende maatregel kan vormen. Deze gebieden worden geïdentificeerd in een risicoanalyse. Voorbeelden zijn:

- technische ruimten waar onrechtmatige toegang veiligheids- of continuïteitsrisico's met zich brengt (bijvoorbeeld ruimten met luchtbehandelingsinstallaties);
- *Main Equipment Rooms* (MER) en *Satellite Equipment Rooms* (SER), waarin (vitale) IT-infrastructuur is opgesteld. Afhankelijk van de ligging en functie van deze ruimten kan sprake zijn van een verhoogd risico op ongeoorloofde toegang of kan het functioneren van vitale voorzieningen direct afhankelijk zijn van de beschikbaarheid en integriteit van deze ruimten;
- locaties waar eerdere incidenten of een concrete dreiging zijn vastgesteld;
- kunstopslag en -galerij;
- opslag van tentamens en IT-apparatuur die tijdens tentamens wordt ingezet;
- opslag van getuigschriften;
- post- en logistieke ruimten;
- Fietsenstallingen.

Dit overzicht is illustratief en niet uitputtend.

4.2.3 Locaties waar cameratoezicht in beginsel niet is toegestaan

Dit zijn locaties waar cameratoezicht in principe niet wordt toegepast, omdat de inbreuk op de persoonlijke levenssfeer zwaar weegt. Het gaat om:

- kantoorgebieden en werkplekken;
- studieplekken en zelfstudieruimten;
- onderwijszalen.

In deze ruimten worden geen camera's geplaatst voor reguliere veiligheidsdoeleinden. Uitsluitend in zeer uitzonderlijke, zwaarwegende gevallen, waarin sprake is van een concrete en specifieke dreiging voor de veiligheid van personen en minder ingrijpende maatregelen onvoldoende effectief zijn, kan hier tijdelijk aanvullend cameratoezicht worden overwogen.

Een dergelijk voorstel wordt behandeld volgens de aanvullende procedure van artikel 4.3, vijfde lid, van het Reglement Cameratoezicht EUR 2026. De aanvraag wordt daarbij beoordeeld door het Toetsingsteam Cameratoezicht en de Functionaris Gegevensbescherming. De maximale duur van een dergelijke inzet bedraagt drie maanden, zonder mogelijkheid tot verlenging of omzetting in permanent cameratoezicht.

Het kan voorkomen dat een camera die is geplaatst op een in paragraaf 4.2.1 of 4.2.2 genoemde locatie, ook (gedeeltelijk) zicht heeft op een werkplek. Dit kan zich bijvoorbeeld voordoen bij een camera in een centrale hal waar zich tevens een horecavoorziening bevindt. In dergelijke gevallen draagt de EUR er zorg voor dat de camera zodanig wordt gepositioneerd dat de werkplek niet structureel in beeld komt. Indien dit niet (volledig) mogelijk is, wordt in de software van het camerasysteem het betreffende deel van het beeld waarin de werkplek zichtbaar is permanent afgeschermd.

4.2.4 Locaties waar cameratoezicht nooit is toegestaan

Tot slot zijn er locaties waar cameratoezicht geheel is uitgesloten, ongeacht de omstandigheden. Deze uitsluiting sluit rechtstreeks aan bij artikel 4.1, vijfde lid Reglement Cameratoezicht EUR 2026. Cameratoezicht vindt hier in geen enkele vorm plaats (permanent, tijdelijk of heimelijk). Het betreft in ieder geval:

- toiletten, douches en kleedruimten;
- ruimtes voor vertrouwelijke gesprekken, zoals spreekkamers of counselingruimtes;
- bijzondere ruimtes zoals stilteruimtes en lactatieruimtes.

Voor deze locaties geldt dat veiligheidsproblemen altijd met andere middelen moeten worden aangepakt, bijvoorbeeld door fysieke aanwezigheid van beveiliging, bouwkundige maatregelen of organisatorische afspraken, en niet via cameratoezicht. Afwijking van deze uitsluiting is op grond van artikel 4.1, vijfde lid, van het Reglement Cameratoezicht EUR 2026 niet mogelijk.

4.3 Externe EUR-locaties (ISS, EUC, C&C Putselaan)

Ook op externe locaties in beheer van de EUR, zoals ISS, EUC en C&C Putselaan, kan cameratoezicht structureel onderdeel zijn van de veiligheidsinrichting. In de basis gelden hiervoor dezelfde uitgangspunten en locatiecategorieën als in dit hoofdstuk zijn beschreven.

De aard en omgeving van deze locaties wijken af van Campus Woudestein: het betreft gebouwen in een stedelijke omgeving, met andere publieke ruimten en gebruiksprofielen. Het Cameraplan voor deze locaties is daarom gebaseerd op een specifieke risicoanalyse per locatie. Op basis daarvan kan de EUR andere keuzes maken in de toepassing van cameratoezicht dan op Campus Woudestein, bijvoorbeeld in de balans tussen camera's aan de buitenzijde en in interne verkeersruimten, mits deze keuzes in lijn zijn met dit beleidskader en worden uitgevoerd volgens de procedures van het Reglement Cameratoezicht EUR 2026.

5 Privacy en waarborgen

Zoals eerder beschreven bestaat er een inherent spanningsveld tussen de inzet van cameratoezicht en de bescherming van de persoonlijke levenssfeer van betrokkenen. De EUR hanteert daarom duidelijke criteria voor het inzetten van cameratoezicht en treft maatregelen om de gevolgen ervan zoveel mogelijk te mitigeren. Deze maatregelen zijn deels gebaseerd op wettelijke verplichtingen en compliance-vereisten, en vloeien deels voort uit de overtuiging dat de EUR zorgvuldig, terughoudend en verantwoord dient om te gaan met de inzet van cameratoezicht.

5.1 Verwerkingsgrondslag

De verwerkingsgrondslag is die van gerechtvaardigd belang (art. 6 lid 1 sub f AVG). Het desbetreffende belang is het zorgen voor een veilig klimaat en het handhaven van de orde in de gebouwen en op de terreinen van de EUR. Op grond hiervan mag het College van Bestuur regels stellen en onder meer voorschrijven dat in bepaalde situaties middelen, zoals cameratoezicht, worden ingezet.² De verwerkingsgrondslag en doeleinden van het cameratoezicht zijn nader uitgewerkt in artikel 1.2 van het Reglement Cameratoezicht EUR 2026. Verwerking en verdere verwerking vindt uitsluitend plaats voor zover dit verenigbaar is met de in het reglement benoemde doeleinden (i.e., doelbinding).

In lijn met de AVG werkt de EUR deze grondslag en de daarbij behorende belangenafweging nader uit in:

- een *Legitimate Interest Assessment* (LIA), waarin de gerechtvaardigde belangen van de EUR worden geïdentificeerd en afgewogen tegen de belangen en rechten van betrokkenen;
- een *Data Protection Impact Assessment* (DPIA), waarin de privacyrisico's van het camerasysteem in kaart worden gebracht en passende mitigerende maatregelen worden vastgesteld.

De LIA en de DPIA hebben betrekking op het cameratoezichtssysteem als geheel en vormen de basis voor de beoordeling van concrete aanvragen voor cameratoezicht.

5.2 Waarborgen

Om de gevolgen van cameratoezicht voor de persoonlijke levenssfeer van studenten, medewerkers en bezoekers te beperken, treft de EUR een samenhangend stelsel van fysieke, technische en organisatorische waarborgen, aangevuld met onafhankelijk toezicht en medezeggenschap.

Tot de fysieke waarborgen behoren de beveiligingsmaatregelen rond de centrale meldkamer en de ruimten waarin de apparatuur van het camerasysteem is ondergebracht. Deze ruimten zijn niet vrij toegankelijk en kunnen slechts door een beperkt aantal geautoriseerde medewerkers worden betreden, waardoor de mogelijkheid om camerabeelden te bekijken tot een kleine groep wordt beperkt. Beeldschermen met live-beelden zijn zo gepositioneerd dat onbevoegd meekijken zo veel mogelijk wordt voorkomen.

² Artikel 7.57h WHW

De technische waarborgen hebben betrekking op de informatiebeveiliging en de inrichting van het camerasysteem. Het camerasysteem voldoet aan de eisen uit het EUR Privacy- en Informatiebeveiligingsbeleid; de diensteenheden RE&F en EDIS borgen gezamenlijk de IT- en informatiebeveiliging. Binnen het camerasysteem wordt gebruikgemaakt van logging en een audittrail, zodat ongeoorloofd gebruik of misbruik van camerabeelden kan worden vastgesteld en achteraf kan worden gecontroleerd. Waar nodig worden delen van het beeld structureel afgeschermd, bijvoorbeeld wanneer werkplekken of andere gevoelige zones in beeld zouden komen.

De EUR hanteert ook bewust niet de in praktijk gebruikelijke bewaartermijn van 28 dagen: wanneer geen incident is geconstateerd, worden beelden automatisch en onomkeerbaar verwijderd na uiterlijk veertien dagen, tenzij sprake is van een incident of een verzoek van een betrokkene als bedoeld in het Reglement Cameratoezicht EUR 2026.

Naast deze actieve technische waarborgen, maakt de EUR ook expliciet geen gebruik van een aantal functionaliteiten van het CCTV-systeem. Zo is de mogelijkheid om audio op te nemen uitgeschakeld in de camera's. Ook maakt de EUR expliciet geen gebruik van AI-toepassingen, zoals gezichtsherkenning of de mogelijkheid om een persoon geautomatiseerd te volgen. Indien het door de EUR gebruikte CCTV-systeem dergelijke functionaliteiten bevat, zijn deze standaard uitgeschakeld en niet beschikbaar voor gebruik. Daarnaast is contractueel bepaald dat leveranciers van het CCTV-systeem geen gegevens van de EUR mogen verwerken voor het trainen van AI-modellen.

De keuze om geen gebruik te maken van AI-toepassingen is een bewuste afweging. Slimme software zou de privacy kunnen verbeteren doordat bijvoorbeeld een camera normaliter 'op zwart' kan staan en de centralist slechts alarmeert wanneer een incident wordt geconstateerd. De EUR ziet op dit moment echter nog te veel risico's, zoals etnisch profileren of onrechtmatige verwerking van persoonsgegevens. Deze risico's wegen voor de EUR nog zwaarder dan de mogelijke voordelen.

Als beperkte uitzondering hierop kan de EUR gebruik maken van intelligente bewegingsdetectie. Deze functionaliteit wordt buiten de openingstijden ingezet om de centralist gericht te attenderen op mogelijke onregelmatigheden. De camera's genereren daarbij alleen een alarm wanneer zij specifieke bewegingen detecteren, zoals de aanwezigheid van personen of voertuigen, en niet bij elke willekeurige verandering in het beeld. De analyse voor deze bewegingsdetectie vindt plaats lokaal in de camera en maakt hiervoor geen gebruik van cloudtoepassingen.

De organisatorische waarborgen hebben betrekking op de toegang tot, het gebruik van en de controle op het camerasysteem. Toegang tot het camerasysteem en tot camerabeelden is beperkt en vastgelegd in een autorisatiematrix, die als bijlage bij dit beleidskader is opgenomen en conform artikel 3.4 van het Reglement Cameratoezicht EUR 2026 wordt beheerd. Slechts een beperkt aantal medewerkers heeft, uit hoofde van zijn functie, toegang tot camerabeelden. Het Hoofd EUR Security beheert de autorisaties, controleert deze periodiek en ziet erop toe dat betrokken medewerkers voorafgaand aan de toegang zijn geïnstrueerd over het juiste gebruik van het camerasysteem en de omgang met persoonsgegevens. Beveiligingsmedewerkers, waaronder de centralisten, worden gescreend voordat zij met het camerasysteem mogen werken en ontvangen gerichte training over het gebruik daarvan. De EUR is terughoudend in het delen van live-beelden en opgenomen beelden met derden; de voorwaarden waaronder inzage en uitgifte zijn toegestaan, zijn vastgelegd in hoofdstuk V van het Reglement Cameratoezicht EUR 2026.

Op het geheel van deze waarborgen en op de naleving van de privacykaders wordt toezicht gehouden door de Chief Privacy Officer (CPO) en de Functionaris Gegevensbescherming (FG), zoals beschreven in hoofdstuk II van het Reglement Cameratoezicht EUR 2026. Zij toetsen onafhankelijk of het cameratoezicht voldoet aan de AVG en de interne privacy- en beveiligingskaders, adviseren over risico's en mitigerende maatregelen, en kunnen audits (laten) uitvoeren op de inrichting en het gebruik van het camerasysteem. Daarbij zien zij er mede op toe dat de maatregelen en belangenafwegingen uit de LIA en de DPIA daadwerkelijk worden toegepast.

Daarnaast vervult de Universiteitsraad een controlerende rol. Het College van Bestuur rapporteert jaarlijks aan de Universiteitsraad over de toepassing van cameratoezicht, waaronder wijzigingen in het cameraplan en de autorisatiematrix, de inzet van tijdelijk aanvullend cameratoezicht en heimelijk cameratoezicht, en de inzage en uitgifte van camerabeelden aan derden, conform de bepalingen in het Reglement.

6 Werking en Evaluatie

6.1 Interpretatie

In gevallen verband houdend met de in dit beleidskader geregelde onderwerpen, waarin dit beleidskader niet voorziet of ingeval dit beleidskader aanleiding geeft tot meervoudige interpretatie, beslist het College van Bestuur.

6.2 Beheer

Dit beleidskader is in beheer bij: Algemene Bestuursdienst, diensteenheid Bestuurlijke Zaken, Team Integrale Veiligheid.

6.3 Vertaling

Wanneer dit beleidskader is vertaald en zich er een geval van strijdigheid tussen de Engelse vertaling en de Nederlandse tekst voordoet, prevaleert de Nederlandse versie.

6.4 Inwerkingtreding, werkingsduur, en evaluatie

Dit beleidskader treedt, na instemming door de Universiteitsraad en vaststelling door het College van Bestuur in werking op 1 oktober 2026.

Dit beleidskader heeft een maximale werkingsduur van uiterlijk vijf jaar en vervalt per 30 juli 2031. Na vier jaar vindt een evaluatie plaats van dit beleidskader op basis waarvan een vernieuwd beleidskader wordt ontwikkeld. Indien de situatie hierom vraagt, kan het College van Bestuur op een eerder moment dan de in het tweede lid genoemde termijn wijzigingen in dit Reglement vaststellen, voor zover de Universiteitsraad met deze wijzigingen heeft ingestemd.

6.5 Citeertitel

Dit beleidskader wordt aangehaald als: Beleidskader Cameratoezicht EUR 2026.

Bijlage 1 – Autorisatiematrix

De volgende soorten autorisaties worden onderscheiden:

- A. het live bekijken van camerabeelden;
- B. het terugkijken van binnen de reguliere opslagtermijn opgeslagen camerabeelden;
- C. het terugkijken van buiten de reguliere opslagtermijn opgeslagen camerabeelden;
- D. het opslaan van camerabeelden buiten de reguliere opslagtermijn conform artikel 3.2 Reglement Cameratoezicht EUR 2026;
- E. het bewerken (onherkenbaar maken of verscherpen van bepaalde onderdelen op beelden, exporteren) van opgeslagen camerabeelden;
- F. het geven van inzage in live camerabeelden aan politie tijdens een incident conform artikel 5.1 Reglement Cameratoezicht EUR 2026;
- G. het geven van inzage en uitgifte van opgeslagen camerabeelden aan derden conform artikel 5.2 Reglement Cameratoezicht EUR 2026;
- H. het geven van inzage in opgeslagen camerabeelden aan betrokkenen conform artikel 5.3 Reglement Cameratoezicht EUR 2026;
- I. het live bekijken van camerabeelden t.b.v. technische controle, onderhoud, aanpassingen en installatie.

De volgende functionarissen hebben uit hoofde van hun functie en/of taken de structurele noodzaak tot een bepaalde toegang tot het camerasysteem en de via het cameratoezicht verkregen camerabeelden en gegevens:

Functionaris	A	B	C	D	E	F	G	H	I
Adviseur Integrale Veiligheid, Hoofd EUR Security	x	x	x	x	x	x	x	x	x
Privacy Officer ABD, CPO, FG	x	x	x						
Operationeel manager EUR Security	x	x		x ³		x			x
Centralist	x	x				x			
Beveiligingsbeambten	x	x							
Functionarissen die technische controle-, onderhouds- of installatiewerkzaamheden uitvoeren t.b.v. het Camerasysteem in dienst van Contractor vallend onder RE&F									x

³ De Operationele manager EUR Security heeft binnen het softwaresysteem de autorisatie om camerabeelden te bewaren buiten de retentieperiode. Dit is puur een uitvoerende rol; de beslissing om camerabeelden voor een langere periode op te slaan wordt altijd genomen door de Adviseur Integrale Veiligheid of het Hoofd EUR Security.